



HEWLETT-PACKARD COMPANY  
Intellectual Property Administration  
P.O. Box 272400  
Fort Collins, Colorado 80527-2400

PATENT APPLICATION

ATTORNEY DOCKET NO. 10017270-1

IN THE  
UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s): Richard Paul TARQUINI et al.

Confirmation No.: 3625

Application No.: 10/001,728

Examiner: Lemma, Samson B.

Filing Date: October 31, 2001

Group Art Unit: 2132

Title: **NODE AND MOBILE DEVICE FOR A MOBILE TELECOMMUNICATIONS NETWORK PROVIDING INTRUSION DETECTION**

Mail Stop Appeal Brief-Patents  
Commissioner For Patents  
PO Box 1450  
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF

Transmitted herewith is the Appeal Brief in this application with respect to the Notice of Appeal filed on November 22, 2005.

The fee for filing this Appeal Brief is (37 CFR 1.17(c)) \$500.00.

(complete (a) or (b) as applicable)

The proceedings herein are for a patent application and the provisions of 37 CFR 1.136(a) apply.

☐ (a) Applicant petitions for an extension of time under 37 CFR 1.136 (fees: 37 CFR 1.17(a)-(d)) for the total number of months checked below:

☐ 1st Month  
\$120

☐ 2nd Month  
\$450

☐ 3rd Month  
\$1020

☐ 4th Month  
\$1590

☐ The extension fee has already been filed in this application.

☒ (b) Applicant believes that no extension of time is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

Please charge to Deposit Account 08-2025 the sum of \$ 500. At any time during the pendency of this application, please charge any fees required or credit any over payment to Deposit Account 08-2025 pursuant to 37 CFR 1.25. Additionally please charge any fees to Deposit Account 08-2025 under 37 CFR 1.16 through 1.21 inclusive, and any other sections in Title 37 of the Code of Federal Regulations that may regulate fees. A duplicate copy of this sheet is enclosed.

☒ I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to:  
Commissioner for Patents, Alexandria, VA 22313-1450  
Date of Deposit: January 23, 2006

OR

☐ I hereby certify that this paper is being transmitted to the Patent and Trademark Office facsimile number (571)273-8300.

Date of facsimile:

Typed Name: Cindy C. Dioso

Signature: Cindy C. Dioso

Respectfully submitted,

Richard Paul TARQUINI et al.

By: James L. Baudino

James L. Baudino

Attorney/Agent for Applicant(s)

Reg No. : 43,486

Date : January 23, 2006

Telephone : (214) 855-7510



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

**APPEAL FROM THE EXAMINER TO THE BOARD  
OF PATENT APPEALS AND INTERFERENCES**

Applicants: Richard Paul Tarquini et al. Confirmation No.: 3625  
Application Serial No.: 10/001,728  
Filed: October 31, 2001  
Title: Node and Mobile Device for a Mobile Telecommunications  
Network Providing Intrusion Detection  
  
Group Art Unit: 2132  
Examiner: Lemma, Samson B.  
  
Docket No.: 10017270-1

**MAIL STOP: APPEAL BRIEF PATENTS**  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, Virginia 22313-1450

Dear Sir:

**APPEAL BRIEF**

Applicants has appealed to the Board of Patent Appeals and Interferences from the decision of the Examiner mailed September 22, 2005, finally rejecting Claims 1-13. Applicants filed a Notice of Appeal on November 22, 2005. Applicants respectfully submit herewith this Appeal Brief with authorization to charge the statutory fee of \$500.00.

01/27/2006 WABDELRI 00000019 082025 10001728  
01 FC:1402 500.00 DA

### **REAL PARTY IN INTEREST**

The present application was assigned to Hewlett-Packard Company as indicated by an assignment from the inventor recorded on March 19, 2002 in the Assignment Records of the United States Patent and Trademark Office at Reel 012728, Frame 0054. The present application was subsequently assigned to Hewlett-Packard Development Company, L.P. as indicated by an assignment from Hewlett-Packard Company recorded on September 30, 2003 in the Assignment Records of the United States Patent and Trademark Office at Reel 014061, Frame 0492.

### **RELATED APPEALS AND INTERFERENCES**

There are no known appeals or interferences that will directly affect or be directly affected by or have a bearing on the Board's decision in this pending appeal.

### **STATUS OF CLAIMS**

Claims 1-13 stand rejected pursuant to a final Office Action mailed September 22, 2005. Claims 1-13 are presented for appeal.

### **STATUS OF AMENDMENTS**

No amendment has been filed subsequent to the mailing of the final Office Action.

### **SUMMARY OF CLAIMED SUBJECT MATTER**

Embodiments of the present invention as defined by independent Claim 1 are directed toward a mobile device (355) operable in a telecommunications network (300) comprising a memory module (274) for storing data in machine readable format for retrieval and execution by a central processing unit (272), and an operating system (275) operable to execute an intrusion detection application (91) stored in the memory module (274). (at least at page 15, lines 3-6 and lines 9-16; and figure 5).

Embodiments of the present invention as defined by independent Claim 11 are directed toward a node (85) of a network (300) for managing an intrusion detection system, the node (85) comprising a memory module (274) for storing data in machine readable format for retrieval and execution by a central processing unit (272), and an operating system (275) comprising a network stack (90) comprising a protocol driver (135) and a media access control driver (145) and operable to execute an intrusion protection system management application (279), the management application (279) operable to receive text-file input (277A-277N) defining a network-exploit rule and convert the text-file input (277A-277N) into a signature file (281A-281N) comprising machine-readable logic representative of an exploit-signature, the node (85) operable to transmit the signature file to a mobile device (281A-281N) over a radio frequency link. (at least page 12, lines 10-14; page 14, lines 13-16; page 15, lines 13 through page 16, line 7; and page 16, lines 25-31).

#### **GROUND OF REJECTION TO BE REVIEWED ON APPEAL**

1. Claims 1 and 3-10 are rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 6,725,377 issued to Kouznetsov (hereinafter “Kouznetsov”).

2. Claims 2 and 11-13 are rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,851,061 issued to Holland III et al. (hereinafter “Holland”) in view of U.S. Patent No. 5,557,742 issued to Smaha et al. (hereinafter “Smaha”).

#### **ARGUMENT**

A. Standard

1. 35 U.S.C. § 102

Under 35 U.S.C. § 102, a claim is anticipated only if each and every element as set forth in the claim is found in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. of California*, 2 U.S.P.Q.2d 1051 (Fed. Cir. 1987); M.P.E.P. § 2131. In addition, “[t]he identical invention must be shown in as complete detail as is contained in the . . .

claims” and “[t]he elements must be arranged as required by the claim.” *Richardson v. Suzuki Motor Co.*, 9 U.S.P.Q.2d 1913, 1920 (Fed. Cir. 1989); *In re Bond*, 15 U.S.P.Q.2d 1566 (Fed. Cir. 1990); M.P.E.P. § 2131.

2. 35 U.S.C. § 103

To establish a *prima facie* case of obviousness under 35 U.S.C. § 103, three basic criteria must be met: First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings; second, there must be a reasonable expectation of success; and finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. *In re Vaeck*, 947 F.2d 488, (Fed. Cir. 1991); M.P.E.P. § 2143. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on applicant’s disclosure. *Id.* Further, the mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination. *In re Mills*, 916 F.2d 680 (Fed. Cir. 1990); M.P.E.P. § 2143.01.

3. Effect of Preamble

During examination, statements in the preamble reciting the purpose or intended use of the claimed invention must be evaluated to determine whether the recited purpose or intended use results in a structural difference (or, in the case of process claims, manipulative difference) between the claimed invention and the prior art. If so, the recitation serves to limit the claim. *See, e.g., In re Otto*, 312 F.2d 937, 938, 136 USPQ 458, 459 (CCPA 1963). Further, a “preamble may provide context for claim construction, particularly where that preamble’s statement of intended use forms the basis for distinguishing the prior art in the patent’s prosecution history.” *Metabolite Labs., Inc. v. Corp. of Amer. Holdings*, 370 F.3d 1354, 1358-62 (Fed. Cir. 2004); M.P.E.P. § 2111.02. *See, also, Catalina Mktg. Int’l v. Coolsavings.com, Inc.*, 289 F.3d 801, 808-09, 62 USPQ2d 1781, 1785 (Fed. Cir. 2002) (“[C]lear reliance on the preamble during prosecution to distinguish the claimed invention from the prior art transforms the

preamble into a claim limitation because such reliance indicates use of the preamble to define, in part, the claimed invention.”).

B. Argument

1. First Ground of Rejection (Claims 1 and 3-10)

Claims 1 and 3-10 are rejected under 35 U.S.C. §102(e) as being anticipated by *Kouznetsov*. Of the rejected claims, Claim 1 is independent. Applicants respectfully submit that *Kouznetsov* does not disclose or even suggest each and every limitation of independent Claim 1. Therefore, Applicants respectfully submit that independent Claim 1, and Claims 3-10 that depend therefrom, are in condition for allowance.

Independent Claim 1 recites a “mobile device operable in a mobile telecommunications network” having “a memory module” and “an operating system operable to execute an intrusion detection application stored in the memory module.” Applicants respectfully submit that *Kouznetsov* does not disclose or even suggest “an intrusion detection application stored in the memory module” of a “mobile device operable in a mobile telecommunications network” as recited by independent Claim 1, nor has the Examiner explicitly identified any such disclosure in *Kouznetsov*.

In the Final Office Action, the Examiner states that “what is argued by the applicant is the limitation which is part of [the] preamble but was not part of the body of the claim.” (Final Office Action, page 2). In rejecting Claims 1 and 3-10, the Examiner further states that “[a]n intended use clause found in the preamble is not afforded the effect of a distinguishing limitation unless the body of the claim sets forth the structure which refers back to, is defined by, or otherwise draws life and breath from the preamble.” (Final Office Action, page 3). Applicants respectfully submit that in Applicants’ response filed June 22, 2005, in response to the Office Action mailed March 24, 2005, Applicants clearly relied on the preamble as a basis for distinguishing over the *Kouznetsov* reference. For example, in Applicants’ response filed June 22, 2005, Applicants stated:

Applicants respectfully submit that *Kouznetsov* does not disclose or even suggest “an intrusion detection application stored in the memory module” of a “mobile device operable in a mobile telecommunications network” as recited by independent Claim 1, nor has the Examiner explicitly identified any such disclosure in *Kouznetsov*. Thus, for at least this reason, *Kouznetsov* does not anticipate independent Claim 1.

(Office Action Response, page 4). Accordingly, Applicants submit that the preamble of independent Claim 1 forms a basis for distinguishing over the *Kousznetsov* reference and, as such, is a claim limitation. Accordingly, Applicants reiterate that *Kousznetsov* does not disclose or even suggest “an intrusion detection application stored in the memory module” of a “mobile device operable in a mobile telecommunications network” as recited by independent Claim 1. Thus, for at least this reason, *Kouznetsov* does not anticipate independent Claim 1.

Therefore, Applicants respectfully submit that independent Claim 1 is clearly patentable over the *Kousznetsov* reference and, accordingly, Claim 1, and Claims 3-10 that depend therefrom, are in condition for allowance.

2. Second Ground of Rejection (Claim 2)

Claim 2 was rejected under 35 U.S.C. §103(a) as being unpatentable over *Holland* in view of *Smaha*. Claim 2 depends from independent Claim 1. As discussed above, Claim 1 is in condition for allowance. Therefore, for at least this reason, Applicants respectfully submit that Claim 2 is in condition for allowance.

Further, as discussed above, independent Claim 1 recites “an intrusion detection application stored in the memory module” of a “mobile device operable in a mobile telecommunications network.” Neither *Holland* nor *Smaha*, alone or in combination, discloses, teaches or suggests at least these limitations, nor did the Examiner rely on either *Holland* or *Smaha* to teach these limitations. Therefore, for at least this reason also, Applicants respectfully submit that Claim 2 is in condition for allowance.

3. Second Ground of Rejection (Claims 11-13)

Claims 11-13 were rejected under 35 U.S.C. §103(a) as being unpatentable over *Holland* in view of *Smaha*. Of the rejected claims, Claim 11 is independent. Applicants respectfully submit that neither *Holland* nor *Smaha*, alone or in combination, discloses, teaches or suggests the limitations of independent Claim 11. Therefore, Claim 11, and Claims 12 and 13 that depend therefrom, are in condition for allowance.

In the Final Office Action, the Examiner appears to admit that *Holland* does not disclose a “management application operable to receive text-file input defining a network-exploit rule and convert the text-file input into a signature file comprising machine-readable logic representative of an exploit-signature, the node operable to transmit the signature file to a mobile device over a radio frequency link” as recited by Claim 11 (Final Office action, page 10). However, the Examiner asserts that *Smaha* purportedly teaches the above-referenced limitations, and that it would have been obvious to combine the purported teachings of *Smaha* with *Holland* (Final Office Action, pages 10 and 11). Applicants respectfully disagree.

In the Final Office action, the Examiner asserts that the misuse engine 30 of *Smaha* “converts the input into events/signature and compare[s] it with the known signatures” (Final Office Action, page 4, and page 11). Applicants respectfully disagree. The Examiner refers to figure 5a of *Smaha* and, in particular, reference numeral 144 of figure 5a which illustrates “convert to event” corresponding to “process inputs” indicated by reference numeral 12 of *Smaha* (Final Office Action, page 4 and page 11; *Smaha*, figure 5a). *Smaha* appears to disclose that the misuse engine 30 of *Smaha* receives process inputs 12 in the form of data and records from security state data source [14], log file data source 16, and audit trail records source 18 (*Smaha*, column 6, lines 1-5, figures 1 and 5a). *Smaha* also appears to disclose that misuse engine 30 converts the process inputs 12 (not inputs received by input mechanism 20 referred to by the Examiner) into events and compares the events to signatures (*Smaha*, column 6, lines 9-11). Thus, *Smaha* appears to disclose that information such as log records and audit records are converted to an “event” (defined as “an instant security state of the system” at column 5,



lines 7-8 of *Smaha*), and then *Smaha* compares the event to a signature. In contrast, Claim 11 recites “an intrusion protection system management application . . . operable to receive text-file input defining a network-exploit rule and convert the text-file input into a signature file comprising machine-readable logic representative of an exploit-signature” (emphasis added). Accordingly, Applicants submit that *Smaha* does not disclose or even suggest, either in the portion referred to by the Examiner or elsewhere in *Smaha*, at least this limitation of Claim 11. To the contrary in *Smaha*, the “convert to event” corresponding to reference numeral 144 of *Smaha* referred to by the Examiner is clearly not a “network-exploit rule,” nor is the information referred to by the Examiner “convert[ed] . . . into a signature file comprising machine readable logic representative of an exploit signature” as recited by Claim 11. Thus, for at least this reason, the Examiner’s rejection of Claim 11 is improper.

In the Final Office action, the Examiner also states “before misuse engine 30 begins processing, however, input mechanism 20 for selectable misuses permits narrowing the scope of analysis to a specified set of misuses meets the recitation that input mechanism sets a network-exploit rule.” (Final Office Action, page 4)(emphasis added). Applicants respectfully disagree. As stated above, *Smaha* appears to disclose that misuse engine 30 converts the process inputs 12 into events and compares the events to signatures (*Smaha*, column 6, lines 9-11). Thus, the process inputs 12 of *Smaha* (e.g., log file data 16, audit trail records 18, and security state data 14) do not “defin[e] a network exploit rule” as recited by Claim 11. To the contrary, the signatures of *Smaha*, against which the process inputs 12 are compared, presumably indicate whether or not a particular process input is, in fact, a network exploit. Accordingly, such process inputs 12 of *Smaha* clearly do not “defin[e] a network exploit rule” as recited by Claim 11. Accordingly, *Smaha* does not disclose, teach or suggest “an intrusion protection system management application . . . operable to receive text-file input defining a network-exploit rule and convert the text-file input into a signature file comprising machine-readable logic representative of an exploit-signature” as recited by independent Claim 11 (emphasis added). Thus, for at least this reason also, the Examiner’s rejection of Claim 11 is improper.

Additionally, Claim 11 recites “the node operable to transmit the signature file to a mobile device over a radio frequency link” (emphasis added). In the Final Office action, the Examiner states that “[o]utput report mechanism 38 may send output reports to one or more of storage device 44, communications link 46, network 48 meets the limitation transmitting signature file to the mobile device over a radio frequency link.” (Final Office Action, page 5). Applicants respectfully disagree. First, contrary to the Examiner’s conclusions, nowhere does *Smaha* disclose, teach or suggest a mobile device. Second, Claim 11 recites that a “signature file [is transmitted] to a mobile device over a radio frequency link” (emphasis added). Instead, *Smaha* appears to disclose, and the Examiner appears to rely on, an output of “an output signal” and an “output report,” neither of which appear to be a “signature file” as recited by Claim 11. Therefore, for at least this reason also, Applicants respectfully submit that the rejection of Claim 11 is improper.

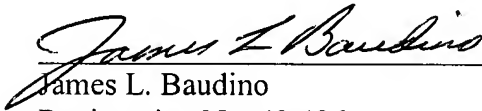
Accordingly, for at least the reasons discussed above, neither *Holland* nor *Smaha*, alone or in combination, discloses, teaches or suggests the limitations of independent Claim 11. Therefore, independent Claim 11, and Claims 12 and 13 that depend therefrom, are clearly patentable over the cited references.

**CONCLUSION**

Applicants have demonstrated that the present invention as claimed is clearly distinguishable over the art cited of record. Therefore, Applicants respectfully request the Board of Patent Appeals and Interferences to reverse the final rejection of the Examiner and instruct the Examiner to issue a notice of allowance of all claims.

The Commissioner is authorized to charge the statutory fee of \$500.00 to Deposit Account No. 08-2025 of Hewlett-Packard Company. Although no other fee is believed due, the Commissioner is hereby authorized to charge any fees or credit any overpayments to Deposit Account No. 08-2025 of Hewlett-Packard Company.

Respectfully submitted,

  
James L. Baudino  
Registration No. 43,486

Date: January 23, 2006

Correspondence To:

L. Joy Griebenow  
Hewlett-Packard Company  
Intellectual Property Administration  
P.O. Box 272400  
Fort Collins, Colorado 80527-2400  
Tel. (970) 898-3884

**CLAIMS APPENDIX**

1. A mobile device operable in a mobile telecommunications network, comprising:
  - a memory module for storing data in machine readable format for retrieval and execution by a central processing unit; and
  - an operating system operable to execute an intrusion detection application stored in the memory module.
2. The mobile device according to claim 1, wherein the operating system further comprises a network stack comprising a protocol driver, a media access control driver, the intrusion detection application comprising an intermediate driver bound to the protocol driver and the media access control driver.
3. The mobile device according to claim 1, wherein the intrusion detection application further comprises an associative process engine and an input/output control layer, the input/output control layer operable to receive a signature file and pass the signature file to the associative process engine, the associative process engine operable to analyze a data packet with the signature file.
4. The mobile device according to claim 1, further comprising a storage media, the storage media operable to maintain a database of a plurality of signature files therein.
5. The mobile device according to claim 3, wherein the intrusion detection application identifies a correspondence between the signature file and a data packet, a determination that the data packet is intrusion-related made upon identification of the correspondence.
6. The mobile device according to claim 3, wherein the signature file comprises a directive that defines a process to be executed by the processor upon a determination that the data packet is intrusion-related.

7. The mobile device according to claim 5, wherein the directive comprises machine readable instructions that, when executed by the processor, cause the mobile device to log the data packet in a database.

8. The mobile device according to claim 1, wherein the intrusion detection application performs host-based intrusion detection by monitoring application logs of applications running on the mobile device.

9. The mobile device according to claim 1, wherein the intrusion detection application is operable to identify an event related to an intrusion of the mobile device, the mobile device operable to provide event-data related to the intrusion to a management node of the network.

10. The mobile device according to claim 9, wherein the management node is a mobile telecommunication network switching system.

11. A node of a network for managing an intrusion detection system, the node comprising:

a memory module for storing data in machine readable format for retrieval and execution by a central processing unit; and

an operating system comprising a network stack comprising a protocol driver and a media access control driver and operable to execute an intrusion protection system management application, the management application operable to receive text-file input defining a network-exploit rule and convert the text-file input into a signature file comprising machine-readable logic representative of an exploit-signature, the node operable to transmit the signature file to a mobile device over a radio frequency link.

12. The node according to claim 11, wherein the radio frequency link is terminated by the mobile device and a base transceiver station of a mobile communications network.

13. The node according to claim 11 further comprising at least one of a visitor location register and a home location register.

**EVIDENCE APPENDIX**

None

**RELATED PROCEEDINGS APPENDIX**

None